Los expertos en ciberseguridad han emitido una advertencia sobre la exposición pública de secretos de configuración de Kubernetes que podría exponer a las organizaciones a riesgos de ataques a la cadena de suministro.

«Estos secretos codificados de configuración de Kubernetes fueron cargados en repositorios públicos», informaron los investigadores de seguridad de Aqua, Yakir Kadkoda y Assaf Morag, en una nueva investigación publicada a principios de esta semana.

Entre las afectadas se encuentran dos destacadas empresas de blockchain y diversas compañías Fortune 500, según la firma de seguridad en la nube. Esta utilizó la API de GitHub para recuperar todas las entradas que contenían los tipos .dockerconfigjson y .dockercfg, que almacenan credenciales para acceder a un registro de imágenes de contenedores.

De los 438 registros que podrían contener credenciales válidas para registros, 203 registros, aproximadamente el 46%, contenían credenciales válidas que permitían el acceso a los registros respectivos. Noventa y tres de las contraseñas fueron establecidas manualmente por individuos, en contraste con las 345 que fueron generadas por computadora.

> *«En la mayoría de los casos, estas credenciales permitían privilegios tanto de extracción como de inserción. Además, con frecuencia encontramos imágenes de contenedores privados dentro de la mayoría de estos registros»,* señalaron los investigadores.

Adicionalmente, cerca del 50% de las 93 contraseñas fueron consideradas débiles, incluyendo términos como *«password», «test123456», «windows12», «ChangeMe» y «dockerhub»,* entre otros.

#	Registry	Counter	Valid Creds (#)	Valid Creds (%)
1	Private registry	135	45	33%
2	Docker Hub	94	64	68%
3	Quay	54	44	81%
4	Azure ECR	24	5	21%
5	GitHub registry	21	10	48%
6	Jfrog	19	4	21%
7	Red hat	17	15	88%
8	Gitlab registry	17	9	53%
9	Aliyun CS	13	3	23%
10	Openshift	10	0	0%
11	GCR	9	0	0%
12	IBM ICR	8	4	50%
13	Harbor	7	0	0%
14	DigitalOcean	4	0	0%
15	Tencent	3	0	0%
16	AWS	1	0	0%
17	OVH	1	0	0%
18	Pivotal	1	0	0%
---	**Sum**	**438**	**203**	**46.3%**

> *«Esto subraya la necesidad crítica de políticas organizativas de contraseñas que apliquen reglas estrictas para la creación de contraseñas y eviten el uso de contraseñas vulnerables»*, añadieron los investigadores.

Aqua también identificó casos en los que las organizaciones no eliminaron secretos de los archivos que se enviaron a repositorios públicos en GitHub, resultando en una exposición

involuntaria.

Pero, en una nota positiva, se descubrió que todas las credenciales asociadas con AWS y Google Container Registry (GCR) eran temporales y caducaron, lo que hacía imposible el acceso. De manera similar, se requería autenticación de dos factores (2FA) en el GitHub Container Registry como una capa adicional contra el acceso no autorizado.

> *«En algunos casos, las claves estaban cifradas y, por lo tanto, no se podía hacer nada con la clave. En algunos casos, aunque la clave era válida, tenía privilegios mínimos, a menudo solo para extraer o descargar un artefacto o imagen específicos»,* explicaron los investigadores.

De acuerdo con el informe sobre el estado de la seguridad de Kubernetes de Red Hat, publicado a principios de este año, las vulnerabilidades y las configuraciones incorrectas se destacaron como las principales preocupaciones de seguridad en entornos de contenedores, con un 37% de los 600 encuestados identificando la pérdida de ingresos/clientes como resultado de un incidente de seguridad relacionado con contenedores y Kubernetes.